A new algorithm for computing class groups of Zariski surfaces

by Jeffrey Lang

2013

Lang, Jeffrey. (2013). A new algorithm for computing class groups of Zariski surfaces. Arabian Journal of Mathematics 2(3):287-293

Published version: http://dx.doi.org/10.1007/s40065-013-0070-5

Arab J Math (2013) 2:287–293
DOI 10.1007/s40065-013-0070-5

Jeffrey Lang

A new algorithm for computing class groups of Zariski surfaces

Received: 7 November 2012 / Accepted: 14 February 2013 / Published online: 6 March 2013

Abstract Let k be an algebraically closed field of characteristic $p \neq 0$ and $X_g \subset A_k^3$ be a normal surface defined by an equation of the form $z^p = g(x, y)$. The two original algorithms for calculating the group of Weil divisors of X_g contain key errors. This paper presents an algorithm that corrects and improves upon the earlier attempts.

Mathematics Subject Classification 13A99

الملخص

ليكن k حقلاً مغلقاً جبرياً مميزه $p \neq 0$ و $X_g \subset A_k^3$ سطحاً ناظمياً معرفاً بمعادلة على الشكل $z^p = g(x,y)$. تتضمن الخوارزميتان الأصليتان لحساب زمرة قواسم وايل لـ X_g أخطاءً رئيسية. تعرض هذه الورقة خوارزمية تصحح وتحسن المحاولات السابقة.

Introduction

Let k be an algebraically closed field of characteristic $p \neq 0$ and $X_g \subset A_k^3$ a normal surface defined by an equation of the form $z^p = g(x, y)$ with $g \in k[x, y]$. Such varieties are known as Zariski surfaces and their divisor class groups have been the focus of much investigation. Although class groups in general are often difficult to determine, for Zariski surfaces they are algorithmically obtainable. [1] and [4] present programmable algorithms for calculating them, but errors were recently discovered in each of these. The first algorithm depends on an incorrect lemma [1, p. 249]. Although it can be repaired, the program is very slow to make it worth while, as it often takes several hours to finish a computation, even for cases of low degree and small characteristic. The second algorithm is more efficient than the original one, but it also contains an error in a critical step [4, pp. 5–6, step 5]. This paper presents a revised version of the latter algorithm that corrects its flaws and provides several computational improvements. Unlike its predecessors, it does not require computing roots, which imposes programming limitations, and it employs for the most part only standard matrix computations already built into most well known mathematical programs. It also differs fundamentally from the recently discovered algorithm introduced in [6] for calculating the divisor class group of a Zariski surface, which involves iteratively calculating a sequence of matrices of increasing size together with their orthogonal complements. The algorithm presented here is computationally simpler in the sense that it only employs elementary row reduction.

J. Lang (✉)
Department of Mathematics, University of Kansas,
Lawrence, Kansas 66045, USA
E-mail: lang@math.ku.edu

1 The isomorphism

Let k be an algebraically closed field of characteristic $p \neq 0$, $g \in k[x, y]$ a polynomial of degree $n \neq 0$ such that g_x and g_y have no common factors in $k[x, y]$, and $X_g \subset A_k^3$ be the surface defined by the equation $z^p = g$. Then X_g is regular in codimension one. Let $Cl\left(X_g\right)$ denote the group of Weil divisors of X_g [3, p. 130].

Theorem 1.1 *Let* $\nabla = \partial^{2p-2}/\partial x^{p-1}\partial y^{p-1}$. *Then* $Cl(X_g)$ *is isomorphic to the additive group* $\mathscr{L}_g = \left\{t \in k[x, y] : \nabla\left(g^i t\right) = 0, 0 \leq i \leq p-2, \nabla\left(g^{p-1}t\right) = t^p\right\}$ *[5, pp. 393–398].*

Corollary 1.2 *If* $t \in \mathscr{L}_g$, *then* $deg\,(t) \leq n-2$.

Proof Since $t^p = \nabla\left(g^{p-1}t\right)$, $pdeg\,(t) \leq (p-1)\,n + deg\,(t) - 2\,(p-1)$, which implies $deg\,(t) \leq n-2$. □

Definition 1.3 For a field F and positive integers r and s, let $F^{r\text{x}s}$ be the set of r x s matrices with entries in F. If $M = \left[a_{ij}\right] \in F^{r\text{x}s}$ and q is an integer, let $M^{(p^q)} = \left[a_{ij}^{p^q}\right]$. I_r will denote the identity matrix in $F^{r\text{x}r}$ and O_{rs} the zero matrix in $F^{r\text{x}s}$. When the context makes plain the dimension of the zero matrix, we will simply denote it by O. If $M \in F^{r\text{x}s}$, let $row\,(M)$ denote the row space of M. For a matrix D, let R_D denote the reduced row-echelon form of D.

Definition 1.4 Let $g \epsilon k[x, y]$ be as above. Let V be the k-vector space of polynomials in $k[x, y]$ of degree at most $n-2$ (where $n = deg\,(g)$) and for each $r = 0, \ldots, p-1$, let W_r be the k-vector space of polynomials in $k\left[x^p, y^p\right]$ of degree at most $(r+1)\,n - 2p$. For $r = 0, \ldots, p-1$, let $T_r : V \to W_r$ be the linear transformation defined by $T_r(f) = \nabla\left(g^r f\right)$ and let $M_{g,r}$ be the matrix of T_r with respect to the monomial bases $\left\{x^i y^j : 0 \leq i + j \leq n-2\right\}$ and $\left\{x^{ip} j^{jp} : 0 \leq i + j \leq \frac{(r+1)n}{p} - 2\right\}$ of V and W_r, respectively. Then $M_{g,r}$ is a $\frac{n_r(n_r-1)}{2}$ x $\frac{n(n-1)}{2}$ matrix with coefficients in k, where n_r is the greatest integer less than or equal to $\frac{(r+1)n}{p}$. In particular, $M_{g,p-1}$ is a square matrix of dimension $\frac{n(n-1)}{2}$.

Lemma 1.5 *Let* $t = \sum_{i+j=0}^{n-2} \alpha_{ij} x^i y^j \in k[x, y]$, *let* $\mathbf{x}_t = \begin{bmatrix} \alpha_{00} \\ \alpha_{10} \\ \alpha_{01} \\ \vdots \end{bmatrix}$ *in* $k^{\frac{n(n-1)}{2}}$. *Then the map* $t \to \mathbf{x}_t$ *maps* $\mathscr{L}_g$ *isomorphically to the group of solutions of the system of equations* $M_{g,i}\mathbf{x} = O, 0 \leq i \leq p-2, M_{g,p-1}\mathbf{x} = \mathbf{x}^p$.

Proof The system $M_{g,i}\mathbf{x} = O, 0 \leq i \leq p-2$, $M_{g,p-1}\mathbf{x} = \mathbf{x}^{(p)}$ is obtained by comparing coefficients on both sides of the equations $\nabla\left(g^i t\right) = 0$, *for* $i = 0, 1, \ldots, p-2$, and $\nabla\left(g^{p-1}t\right) = t^p$ in (1.1). Thus t is a solution of the differential equations if and only if $\mathbf{x}_t$ is a solution of the matrix equations. The map is also clearly additive. □

Notation 1.6 Hereafter, for $g \in k[x, y]$, let $A_g = \begin{bmatrix} M_{g,0} \\ \vdots \\ M_{g,p-2} \end{bmatrix}$ and $B_g = M_{g,p-1}$, where the $M_{g,i}$ are as in (1.4). By (1.4), $Cl\left(X_g\right)$ is isomorphic to the group of solutions of the system, $A_g\mathbf{x} = O$, $B_g\mathbf{x} = \mathbf{x}^p$.

2 Linearized systems of exponent one

A linearized system of exponent one is a system of equations of the form,

$$A\mathbf{x} = O;\ B\mathbf{x} = C\mathbf{x}^{(p)} \tag{2.1}$$

where $A \in k^{s\text{x}r}$, $B, C \in k^{t\text{x}r}$, for some $r, s, t \in \mathbb{N}$. The solutions to 2.1 form an additive p-group of exponent one (i.e. every non-identity element has order p).

Proposition 2.2 *If* $s + t = r$ *and the rows of* $\begin{bmatrix} C \\ A^{(p)} \end{bmatrix}$ *are independent, then the solution set of 2.1 has finite order.*

Proof Let $R = k[x_1, \ldots, x_r]$ with the relations $O = A^p\mathbf{x}^{(p)}$; $B\mathbf{x} = C\mathbf{x}^p$. Since $det\left(\begin{bmatrix} C \\ A^{(p)} \end{bmatrix}\right) \neq 0$, this system is equivalent to a system of the form $D\mathbf{x} = \mathbf{x}^{(p)}$, for some $D \in k^{rxr}$. Thus R is generated by the monomials $x_1^{e_1} \cdots x_r^{e_r}$ with each $e_i < p$. In particular, R is finite dimensional over k, hence is Artinian, hence has only finitely many maximal ideals. Therefore, $O = A^{(p)}\mathbf{x}^{(p)}$; $B\mathbf{x} = C\mathbf{x}^{(p)}$, and 2.1, have only finitely many solutions. □

Corollary 2.3 *Let A_g and B_g be as in Notation 1.6. Then the solution set of the system $A_g\mathbf{x} = O$, $B_g\mathbf{x} = \mathbf{x}^p$ has order at most $p^{\frac{n(n-1)}{2}}$.*

Proof By Proposition 2.2, $B_g\mathbf{x} = \mathbf{x}^p$, has only finitely many solutions, which by Bezout's theorem is at most $p^{\frac{n(n-1)}{2}}$. □

Proposition 2.4 *If $s + t < r$, then the system in 2.1 has an infinite solution set.*

Proof If $A \neq O$, then one of the variables in 2.1 is a linear combination of the others and the system can be reduced to one of the same form but with one less variable and at least one less equation. Thus, by induction we may assume the system in 2.1 is only of the form, $B\mathbf{x} = C\mathbf{x}^{(p)}$. If the rows of B or C are dependent, then we can either eliminate an equation from the system or replace one with a linear homogeneous equation. So we may assume the rows of B and C are independent and $1 \leq t < r$. After adding a general choice of $r - t - 1$ equations of the form, $\sum_{i=0}^{r} \alpha_i x_i = \sum_{i=0}^{r} \beta_i x_i^p$, to the system, we may also assume $t = r - 1$. If the system has only finitely many solutions, then for a general choice of linear homogeneous form h in the x_i we have: (i) the row vector corresponding to h is independent of the rows of B; (ii) the row vector corresponding to h^p is independent of the rows of C; (iii) the hyperplane, $h = 0$, passes through none of the solution points of the system except the origin. Then by (i) and (ii), the system, $B\mathbf{x} = C\mathbf{x}^{(p)}$; $h = 0$, is such that each solution has multiplicity one and it has no intersections at infinity, which implies by Bezout's theorem that it has p^{r-1} distinct solutions, which contradicts (iii). □

Corollary 2.5 *If the system in 2.1 has only finitely many solutions and the rows of $\begin{bmatrix} A \\ B \end{bmatrix}$ are independent, then $s + t = r$.*

Proof By Proposition 2.4, $r \leq s + t = rank\left(\begin{bmatrix} A \\ B \end{bmatrix}\right) \leq r$. □

Proposition 2.6 *If $s + t = r$ and the rows of $\begin{bmatrix} A \\ B \end{bmatrix}$ and of $\begin{bmatrix} C \\ A^{(p)} \end{bmatrix}$ are independent, then the solution set of 2.1 has order p^t.*

Proof If $\mathbf{x}_0$ is a solution to 2.1, then the system remains fixed under the change of coordinates $\mathbf{x} - \mathbf{x}_0$. Hence, all solutions have the same multiplicity, which is one since $det\left(\begin{bmatrix} A \\ B \end{bmatrix}\right) \neq 0$. Also, 2.1 has no intersections at infinity since $det\left(\begin{bmatrix} C \\ A^{(p)} \end{bmatrix}\right) \neq 0$. By Bezout's theorem, 2.1 has p^t distinct solutions. □

Definition 2.7 Let $A \in k^{sxr}$, $B, C \in k^{txr}$ and $M = \begin{bmatrix} A & O \\ B & C \end{bmatrix}$ form the block matrix $H_1 = \begin{bmatrix} A' \\ B \end{bmatrix}$, where A' is the reduced row-echelon form of A but with the zero rows deleted. Use row operations on H_1 to eliminate all nonzero entries below the pivot entries of A' to obtain an equivalent block matrix $H_2 = \begin{bmatrix} A' \\ B' \end{bmatrix}$ with $row(A') \cap row(B') = \{0\}$. Put the matrix $\begin{bmatrix} B' & C \end{bmatrix}$ in reduced row-echelon form to obtain an equivalent block matrix $\begin{bmatrix} R_{B'} & C' \end{bmatrix}$ (see Definition 1.3). Let B'' be the matrix consisting of the nonzero rows of $R_{B'}$. Then the rows of B'' are independent and $\begin{bmatrix} R_{B'} & C' \end{bmatrix} = \begin{bmatrix} B'' & C'' \\ O & D \end{bmatrix}$ for matrices C'' and D. Let $H_3 = \begin{bmatrix} D \\ A^{(p)} \end{bmatrix}$ and form the block matrix $H_4 = \begin{bmatrix} C'' \\ H_3' \end{bmatrix}$, where H_3' consists of the nonzero rows of R_{H_3}. Use row operations

on H_4 to eliminate all nonzero entries above the pivot entries of H_3' to obtain a block matrix $H_5 = \begin{bmatrix} C''' \\ H_3' \end{bmatrix}$ with $row\left(H_3'\right) \cap row\left(C'''\right) = \{0\}$. Use row operations on $\begin{bmatrix} B'' & C''' \end{bmatrix}$ to obtain an equivalent block matrix $\begin{bmatrix} B''' & R_{C'''} \end{bmatrix}$. Note the rows of B''' are independent. $\begin{bmatrix} B''' & R_{C'''} \end{bmatrix}$ can be written in block form $\begin{bmatrix} \overline{B} & \overline{C} \\ E & O \end{bmatrix}$, where $\overline{C}$ consists of the nonzero rows of $R_{C'''}$, all of the blocks have r columns, $\overline{B}$ and $\overline{C}$ have the same number of rows, O represents the zero block of appropriate dimension, and the rows of $\begin{bmatrix} \overline{B} \\ E \end{bmatrix}$ and the rows of $\overline{C}$ are independent. Define $\overline{M} = \begin{bmatrix} \overline{A} & O \\ \overline{B} & \overline{C} \end{bmatrix}$, where $\overline{A} = \begin{bmatrix} \left(H_3'\right)^{\left(\frac{1}{p}\right)} \\ E \end{bmatrix}$.

Remark 2.8 The number of rows of $\begin{bmatrix} \overline{B} & \overline{C} \end{bmatrix}$ in Corollary 2.5 is clearly less than or equal to the number of rows of $\begin{bmatrix} B & C \end{bmatrix}$.

Proposition 2.9 *Let $A \in k^{s\times r}, B, C \in k^{t\times r}$ and $M = \begin{bmatrix} A & O \\ B & C \end{bmatrix}$. Let $\overline{M} = \begin{bmatrix} \overline{A} & O \\ \overline{B} & \overline{C} \end{bmatrix}$ be as defined in Definition 2.7. Then the solution set of the system, $A\mathbf{x} = O, B\mathbf{x} = C\mathbf{x}^{(p)}$ is identical to that of the system, $\overline{A}\mathbf{x} = 0, \overline{B}\mathbf{x} = \overline{C}\mathbf{x}^{(p)}$.*

Proof The solution set of the system $A\mathbf{x} = O, B\mathbf{x} = C\mathbf{x}^{(p)}$ is clearly identical to that of $A\mathbf{x} = O, B\mathbf{x} = C\mathbf{x}^{(p)}, O = A^{(p)}\mathbf{x}^{(p)}$ and each of the matrices obtained above corresponds to performing elementary operations on this system. □

Proposition 2.10 *Let $A \in k^{s\times r}, B, C \in k^{t\times r}$ and $M = \begin{bmatrix} A & O \\ B & C \end{bmatrix}$. Let $\overline{M} = \begin{bmatrix} \overline{A} & O \\ \overline{B} & \overline{C} \end{bmatrix}$ be as defined in Definition 2.7. Suppose that the matrices $\begin{bmatrix} B & C \end{bmatrix}$ and $\begin{bmatrix} \overline{B} & \overline{C} \end{bmatrix}$ have the same number of rows and the system, $A\mathbf{x} = O, B\mathbf{x} = C\mathbf{x}^{(p)}$, has only finitely many distinct solutions. Then the solution set of the system, $A\mathbf{x} = O, B\mathbf{x} = C\mathbf{x}^{(p)}$, is a p-group of type $(p, \ldots, p)$ of order p^t.*

Proof Replacing A by A' as defined in Definition 2.7, we may assume that the rows of A are independent. Then $\begin{bmatrix} B & C \end{bmatrix}$ *and* $\begin{bmatrix} \overline{B} & \overline{C} \end{bmatrix}$ have the same number of rows if and only if the rows of $\begin{bmatrix} A \\ B \end{bmatrix}$ and the rows of $\begin{bmatrix} C \\ A^{(p)} \end{bmatrix}$ are independent. Then by Corollary 2.5 and Proposition 2.6, the system, $A\mathbf{x} = O, B\mathbf{x} = C\mathbf{x}^{(p)}$, has exactly p^t distinct solutions. Since the solution set is a finite abelian group with every nonzero element having order p, the rest of the conclusion follows. □

3 The algorithm

Proposition 3.1 *Let $A \in k^{s\times r}, B, C \in k^{t\times r}$ Let $M_0 = \begin{bmatrix} A_0 & O \\ B_0 & C_0 \end{bmatrix} = M = \begin{bmatrix} A & O \\ B & C \end{bmatrix}$ and for each $i = 0, 1, 2, \ldots$, let $M_{i+1} = \begin{bmatrix} A_{i+1} & O \\ B_{i+1} & C_{i+1} \end{bmatrix} = \left[\overline{M_i}\right] = \begin{bmatrix} \overline{A_i} & O \\ \overline{B_i} & \overline{C_i} \end{bmatrix}$ as defined in Definition 2.7. If $\begin{bmatrix} B_j & C_j \end{bmatrix}$ and $\begin{bmatrix} B_{j+1} & C_{j+1} \end{bmatrix}$ have the same numbers of rows, then $\begin{bmatrix} B_j & C_j \end{bmatrix}$ and $\begin{bmatrix} B_{j+e} & C_{j+e} \end{bmatrix}$ will have the same number of rows for all $e \geq 1$.*

Proof As in the proof of Proposition 2.10, after replacing A_j by A_j', we may assume that the rows of A_j are independent. Then $\begin{bmatrix} B_j & C_j \end{bmatrix}$ and $\begin{bmatrix} \overline{B_j} & \overline{C_j} \end{bmatrix}$ have the same number of rows if and only if the rows of $\begin{bmatrix} A_j \\ B_j \end{bmatrix}$ and the rows of $\begin{bmatrix} C_j \\ A_j^{(p)} \end{bmatrix}$ are independent. Hence, $\overline{A}_j$ as defined in Definition 2.7 will be R_{A_j} (see Definiton 1.3), $\overline{B}_j$ will be row equivalent to $R_{B_j'}$, and $\overline{C}_j$ will be $R_{C_j'''}$, where B_j' and C_j''' are as described in Definition 2.7, and the row operations that create these matrices will produce no zero rows. From this, it follows that the rows

of the matrices $\begin{bmatrix} A_{j+1} \\ B_{j+1} \end{bmatrix} = \begin{bmatrix} \overline{A}_j \\ \overline{B}_j \end{bmatrix}$ and $\begin{bmatrix} C_{j+1} \\ A_{j+1}^{(p)} \end{bmatrix} = \begin{bmatrix} \overline{C}_j \\ \overline{A}_j^{(p)} \end{bmatrix}$ will be independent and, in fact, $M_{j+1} = M_{j+e}$, for all $e \geq 1$. □

Corollary 3.2 *Let $A \in k^{sxr}$, $B, C \in k^{txr}$, $M_i = \begin{bmatrix} A_i & O \\ B_i & C_i \end{bmatrix}$ be as in Proposition 3.1, and let i_0 be minimal such that $\begin{bmatrix} B_{i_0} & C_{i_0} \end{bmatrix}$ and $\begin{bmatrix} B_{i_0+1} & C_{i_0+1} \end{bmatrix}$ have the same number of rows. If the system, $A\mathbf{x} = O$, $B\mathbf{x} = C\mathbf{x}^{(p)}$, has only finitely many distinct solutions, then its solution set is a p-group of type $(p, \ldots, p)$ of order p^m, where m is the number of rows of $\begin{bmatrix} C_i & D_i \end{bmatrix}$ for any $i \geq i_0$.*

Proof By Proposition 3.1, if $i \geq i_0$, then $\begin{bmatrix} C_i & D_i \end{bmatrix}$ and $\begin{bmatrix} \overline{C}_i & \overline{D}_i \end{bmatrix}$ have the same number of rows. Hence, $\begin{bmatrix} A_i \\ B_i \end{bmatrix}$ and $\begin{bmatrix} C_i \\ A_i^{(p)} \end{bmatrix}$ have independent rows. The conclusion follows by Proposition 2.10. □

Proposition 3.3 *Let $A \in k^{sxr}$, $B, C \in k^{txr}$, $M_i = \begin{bmatrix} A_i & O \\ B_i & C_i \end{bmatrix}$ be as in Proposition 3.1, and let i_0 be minimal such that $\begin{bmatrix} B_{i_0} & C_{i_0} \end{bmatrix}$ and $\begin{bmatrix} B_{i_0+1} & C_{i_0+1} \end{bmatrix}$ have the same number of rows. Then $i_0 \leq 1 + min\left\{rank\left(\begin{bmatrix} A \\ B \end{bmatrix}\right), rank\left(\begin{bmatrix} C \\ A^{(p)} \end{bmatrix}\right)\right\} - rank\,(A)$.*

Proof In Definition 2.7 we have $rank\left(A'\right) = rank\,(A)$ and $row\left(A'\right) \cap row\left(B'\right) = \{0\}$. Thus, $rank\left(\overline{B}\right) \leq rank\left(B'''\right) = rank\left(B''\right) = rank\left(R'_B\right) = rank\left(B'\right) = rank\left(\begin{bmatrix} A \\ B \end{bmatrix}\right) - rank\,(A)$. Similarly, $rank\left(\overline{C}\right) \leq rank\left(\begin{bmatrix} C \\ A^{(p)} \end{bmatrix}\right) - rank\,(A)$. Since the numbers of rows of $\overline{B}$ and $\overline{C}$ are equal to their ranks, the number of rows of $\begin{bmatrix} \overline{B} & \overline{C} \end{bmatrix}$ is less than or equal to $min\left\{rank\left(\begin{bmatrix} A \\ B \end{bmatrix}\right), rank\left(\begin{bmatrix} C \\ A^{(p)} \end{bmatrix}\right)\right\} - rank\,(A)$. The conclusion then follows from Remark 2.8. □

Algorithm I for Calculating$Cl\left(X_g\right)$ 3.4 The above results provide an algorithm for calculating the order of the solution set of a system $A\mathbf{x} = O$, $B\mathbf{x} = C\mathbf{x}^{(p)}$ when the order is finite. Simply recursively calculate M_i until the number of rows of $\begin{bmatrix} B_i & C_i \end{bmatrix}$ stabilizes. Proposition 3.3 provides an upper bound for the number of required steps. The order of the solution set is then p^m, where m is the stabilization number. A drawback to this is that with each loop in the algorithm p^{th} roots of increasing exponent are introduced, which could slow computations. It would be more convenient if this could be avoided, which is the purpose of the next result.

Definition 3.5 Let $A \in k^{sxr}$, $B, C \in k^{txr}$ and $M = \begin{bmatrix} A & O \\ B & C \end{bmatrix}$. Let $\overline{M} = \begin{bmatrix} \overline{A} & \overline{O} \\ \overline{B} & \overline{C} \end{bmatrix}$ be as in Definition 2.7. Define $\widehat{M} = \overline{M}^{(p)} = \begin{bmatrix} \overline{A}^{(p)} & O \\ \overline{B}^{(p)} & \overline{C}^{(p)} \end{bmatrix} = \begin{bmatrix} \widehat{A} & 0 \\ \widehat{B} & \widehat{C} \end{bmatrix}$. Then $\widehat{A} = \begin{bmatrix} H'_3 \\ E^{(p)} \end{bmatrix}$, where H'_3 and E are described in Definition 2.7.

Proposition 3.6 *Let $A \in k^{sxr}$, $B, C \in k^{txr}$. Let $\widetilde{M}_0 = \begin{bmatrix} \widetilde{A}_0 & O \\ \widetilde{B}_0 & \widetilde{C}_0 \end{bmatrix} = M = \begin{bmatrix} A & O \\ B & C \end{bmatrix}$ and for each $i = 0, 1, 2, \ldots$, let $\widetilde{M}_{i+1} = \begin{bmatrix} \widetilde{A}_{i+1} & O \\ \widetilde{B}_{i+1} & \widetilde{C}_{i+1} \end{bmatrix} = \left[\widehat{M}_i\right] = \begin{bmatrix} \widehat{A}_i & O \\ \widehat{B}_i & \widehat{C}_i \end{bmatrix}$ as defined in Definition 3.5. Then for each $i = 0, 1, 2, \ldots, \widetilde{M}_i = M_i^{(p^i)}$, with M_i as in Proposition 3.1.*

Proof The proof is by a simple induction on i and the fact that applying the Frobenius map to the entries of a matrix commutes with elementary row operations. □

Algorithm II for Calculating$Cl\left(X_g\right)$ 3.7 Let $g \in k[x, y]$ be of degree $n \neq 0$ such that g_x and g_y have no common factors in $k[x, y]$. The following steps calculate $Cl\left(X_g\right)$. Let $A_0 = A_g$, $B_0 = B_g$ and $C_0 = I$, the

identity matrix of dimension $\frac{n(n-1)}{2}$. Then for each $i = 0, 1, 2, \ldots$, calculate $\widehat{M}_i = \begin{bmatrix} \widehat{A}_i & O \\ \widehat{B}_i & \widehat{C}_i \end{bmatrix}$ as in Definition 3.5 until the number of rows of $\begin{bmatrix} \widehat{B}_i & \widehat{C}_i \end{bmatrix}$ stabilizes. Then $Cl(X_g)$ is a p-group of type $(p, \ldots, p)$ of order p^m, where m is the stabilization number.

Remark 3.8 All of the steps in Algorithm II for calculating $Cl\,(X_g)$ 3.7 involve easily programmable steps (e.g. computing $M^{(p)}$ for a matrix M), or apply simple procedures already built into computational software programs (e.g. putting a matrix in reduced row-echelon form), or can be readily adapted to built in programs. The latter includes the steps of eliminating all entries in $\begin{bmatrix} A \\ B \end{bmatrix}$ below the pivot elements of a matrix A that is in reduced row-echelon form. If $A \in k^{sxr}$ is in reduced row-echelon form and $B \in k^{txr}$, then to eliminate all entries in $\begin{bmatrix} A \\ B \end{bmatrix}$ below the pivot elements of A, let B^* be obtained from B by deleting the columns of the latter that do not contain pivot elements of A. Let $J = I_{s+t} + \begin{bmatrix} O & O \\ -B^* & O \end{bmatrix}$. Then $J \begin{bmatrix} A \\ B \end{bmatrix}$ will have the desired form.

Example 3.9 Let k be an algebraically closed field of characteristic 3, $g = x + y + x^2 + y^2 + x^2y + xy^2 + x^4 + xy^3 + 2y^4$, and $X_g \subset A^3_k$ the surface defined by $z^p = g$. We have $A_g = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix}$ and

$$B_g = \begin{bmatrix} 0 & 2 & 2 & 1 & 2 & 1 \\ 2 & 0 & 0 & 2 & 1 & 2 \\ 0 & 2 & 2 & 1 & 2 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}.$$

As in Algorithm II for calculating $Cl\,(X_g)$ 3.7 $A_0 = A_g$, $B_0 = B_g$, $C_0 = I_6$. We then have

$$A_1 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 2 & 0 & 0 & 2 & 1 & 0 \end{bmatrix}, \quad \begin{bmatrix} B_1 & C_1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 1 & 2 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 2 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

and

$$A_2 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 2 & 2 \end{bmatrix}, \quad \begin{bmatrix} B_2 & C_2 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 2 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}$$

Then $A_3 = A_2$ and $\begin{bmatrix} B_3 & C_3 \end{bmatrix} = \begin{bmatrix} B_2 & C_2 \end{bmatrix}$, which implies $Cl\,(X_g)$ has order p^2; i.e. $Cl\,(X_g) \cong \mathbb{Z}_p \oplus \mathbb{Z}_p$.

Example 3.10 Let k be an algebraically closed field of characteristic 3, $g = x + y + x^2 + 2xy + 2y^2 + 2xy^2 + x^4 + 2xy^3 + 2y^4$, and $X_g \subset A^3_k$ the surface defined by $z^p = g$. We have$A_g = \begin{bmatrix} 0 & 2 & 0 & 2 & 2 & 1 \end{bmatrix}$ and

$$B_g = \begin{bmatrix} 0 & 2 & 0 & 1 & 2 & 1 \\ 1 & 1 & 1 & 1 & 2 & 2 \\ 2 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 2 & 1 \end{bmatrix}.$$

As in Algorithm II for calculating $Cl\,(X_g)$ 3.7 $A_0 = A_g$, $B_0 = B_g$, $C_0 = I_6$. We then have

$$A_1 = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 2 \\ 0 & 0 & 1 & 1 & 2 & 0 \end{bmatrix}, \quad \begin{bmatrix} B_1 & C_1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 2 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix},$$

$$A_2 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 2 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 2 \end{bmatrix}, \quad [B_2\ C_2] = \begin{bmatrix} 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix},$$

and

$$A_3 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 2 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 2 \end{bmatrix}, \quad [B_3\ C_3] = [0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 2\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1].$$

Then $A_4 = A_3$ and $[B_4\ C_4] = [B_3\ C_3]$, which implies $Cl(X_g)$ has order p; i.e. $Cl(X_g) \cong \mathbb{Z}_p$.

Remark 3.11 The algorithm presented above Algorithm II for calculating $Cl(X_g)$ 3.7 determines $Cl(X_g)$ up to isomorphism by calculating the order of the additive group of solutions of the system $A_g\mathbf{x} = O$, $B_g\mathbf{x} = \mathbf{x}^p$. Obtaining a set of actual divisors that generate $Cl(X_g)$ requires calculating the group of solutions to $A_g\mathbf{x} = O$, $B_g\mathbf{x} = \mathbf{x}^p$. This can be done algorithmically but we have not yet found a way to do this efficiently, which is a current project.

References

1. Blass, P.; Joyce, D.; Lang, J.: The divisor classes of the surface $z^{p^m} = G(x, y)$, a programmable problem. J. Algebra **100** (1986)
2. Blass, P.; Lang, J.: Zariski Surfaces and Differential equations in Characteristic $p > 0$. Dekker, New York (1987)
3. Hartshorne, R.: Algebraic Geometry. Springer, New York (1977)
4. Lang, J.; Rogers, C.: Applications of a new algorithm for computing class groups of Zariski Surfaces. Ulam Quarterly Vol. 3, No. 3. (1997)
5. Lang, J.: The divisor class group of the surface $z^{p^n} = G(x, y)$ over fields of characteristic $p > 0$. J. Algebra **84** (1983)
6. Lang, J.: Zariski surfaces, class groups and linearized systems. J. Pure Appl. Algebra **215** (2011)
7. Samuel, P.: Lectures on unique factorization domains, in Tata Lecture Notes. Tata Inst. Fundamental Res., Bombay (1964)